

CLAIMS

1. A method for verifying the identity of a message-originator program (D) by a message-receiver program (S), the method comprising the steps of:

- receiving from said message-originator program (D) a message comprising a program-specific identifier ($H(D)$), which has been provided for said message-originator program (D) by means of a trusted computing base (TCB); and
- verifying whether said received program-specific identifier ($H(D)$) is known to said message-receiver program (S).

2. A method for disclosing the identity of a message-originator program (D) to a message-receiver program (S), the method comprising:

- sending from said message-originator program (D) to said message-receiver program (S) a message comprising a program-specific identifier ($H(D)$), which has been provided for said message-originator program (D) by means of a trusted computing base (TCB), said program-specific identifier ($H(D)$) being verifiable at said message-receiver program (S) whether it is known to said message-receiver program (S).

3. A method for verifying the identity of a message-originator program (D) by a message-receiver program (S), the method comprising the steps of:

- providing a program-specific identifier ($H(D)$) for said message-originator program (D) by means of a trusted computing base (TCB);
- sending from said message-originator program (D) to said message-receiver program (S) a message comprising said program-specific identifier ($H(D)$);
- receiving at said message-receiver program (S) said message; and

- verifying whether said received program-specific identifier ($H(D)$) is known to said message-receiver program (S).
4. Method according to claim 1, wherein the message-receiver program (S) afterwards becomes a response-message-originator program and sends a response-message to the message-originator program (D) comprising:
- 5
- a response-program-specific identifier ($H(S)$), which has been provided for said response-message-originator program by means of the trusted computing base (TCB); and
 - an acknowledgment if the program-specific identifier ($H(D)$) has been verified as
- 10 being known.
5. Method according to claim 1, wherein a substantially unique cryptographic identifier that is derived by applying a cryptographic function (H) to the message-originator program (D), preferably a hash function, and more preferably a one-way-hash function, such as MD5 or SHA-1, is used as the program-specific identifier ($H(D)$).
- 15 6. Method according to claim 1, further comprising the step of signing the program-specific identifier ($H(D)$) and/or the message by use of a private cryptographic key (k^{-1}) to establish trust between different programs.
7. Method according to claim 6, wherein the message further comprises an additional program-specific identifier ($H(G)$) that is signed by use of the private cryptographic
- 20 key (k^{-1}) to establish a membership of an additional program in a trust relationship.
8. Method according to claim 1, wherein the message-receiver program (S) has a public cryptographic key (k).

- 5 9. Method according to claim 1, wherein the message-receiver program (S) and/or the trusted computing base (TCB) use(s) a list comprising pre-stored program-specific identifiers and wherein said message-receiver program (S) verifies whether the program-specific identifier ($H(D)$) is identical to one of said pre-stored program-specific identifiers.
10. Method according to claim 1, wherein the message-receiver program (S) sends a rejection-message if the program-specific identifier ($H(D)$) is not verified as being known.
- 10 11. Method according to claim 1, wherein the message-originator program (D) and the message-receiver program (S) are executed on different systems and are connectable via a network, each having its trusted computing base (TCB) for providing program-specific cryptographic identifiers.
12. A computer program comprising program code means for performing the steps of claim 1, when said program is run on a computer.
- 15 13. A computer program product comprising program code means stored on a computer readable medium for performing the method of claim 1, when said program product is run on a computer.
14. An apparatus for verifying the identity of a message-originator program (D) by a message-receiver program (S) on a computer, the apparatus comprising:
- 20 - computing means;
- a receiver-module for receiving from said message-originator program (D) a message comprising a program-specific identifier ($H(D)$), which has been provided

- 25 -

for said message-originator program (D) by means of a trusted computing base (TCB); and

- a verifier-module that verifies whether said program-specific identifier ($H(D)$) is known to said message-receiver program (S).

5 15. An apparatus for disclosing the identity of a message-originator program (D) by a message-receiver program (S) on a computer, the apparatus comprising:

- computing means;
- a trusted computing base (TCB) comprising a generator-module for creating a program-specific identifier ($H(D)$); and
- 10 - a sender-module for sending from said message-originator program (D) a message comprising said program-specific identifier ($H(D)$), said program-specific identifier ($H(D)$) being verifiable at said message-receiver program (S) whether it is known to said message-receiver program (S).

15

* * *